(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11194709 A**

(43) Date of publication of application: **21 . 07 . 99**

(51) Int. Cl **G09C 1/00**
G09C 5/00
H04L 9/32
H04N 1/387
H04N 1/40

(21) Application number: **10000875**

(22) Date of filing: **06 . 01 . 98**

(71) Applicant: **NTT DATA CORP**

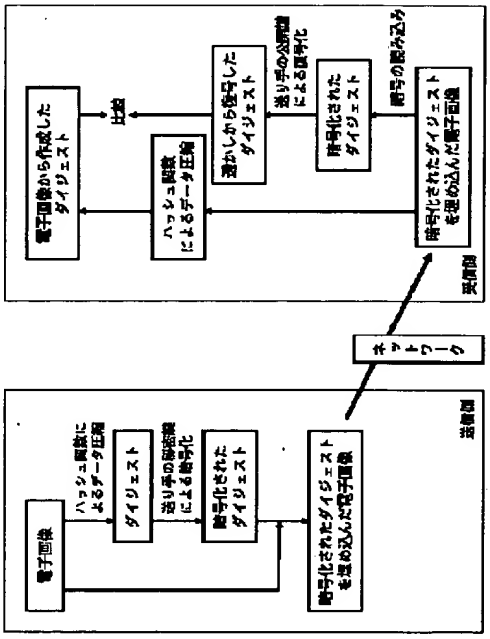
(72) Inventor: **YAMAOKA MASATERU**
KONISHI KAZUYA

(54) **METHOD OF ELECTRONIC AUTHENTICATION AND SYSTEM THEREOF**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a method of electronic authentication permitting an exact electronic authentication at a receiver side without much change in an electronic image between before and after embedding the information at a transmitter side.

SOLUTION: At a transmitter side, a digest is made from a high-ranking bits of an electronic image where one pixel is expressed by predetermined bits, and is enciphered by using sender's private key and embedded in each pixel's lower-ranking bits for being transmitted to a network. At a receiver side, the coded digest read out from the transmitted electronic image is decoded by the sender's public key, and authentication of the electronic image is executed by comparing and checking this decoded digest with a checking use digest directly generated from the transmitted electronic image.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－194709

(43)公開日　平成11年(1999)７月21日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ｂ
	5/00			5/00	
Ｈ０４Ｌ	9/32		Ｈ０４Ｎ	1/387	
Ｈ０４Ｎ	1/387		Ｈ０４Ｌ	9/00	６７５Ｂ
	1/40		Ｈ０４Ｎ	1/40	Ｚ

審査請求　未請求　請求項の数８　ＯＬ　（全９頁）

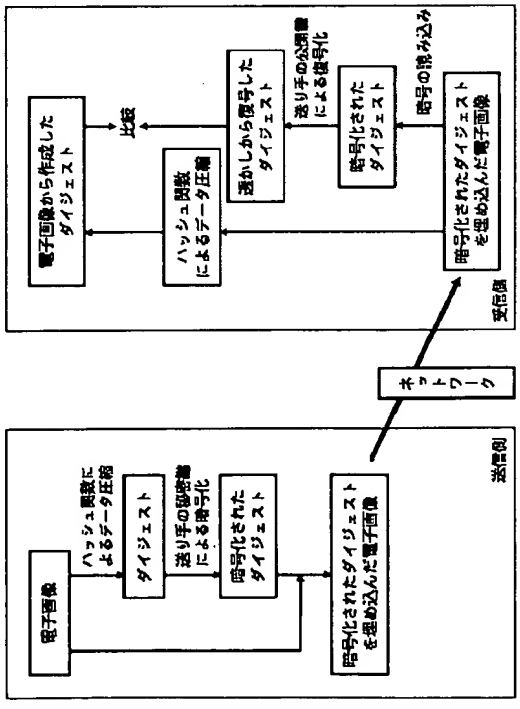
(21)出願番号　特願平10－875

(22)出願日　平成10年(1998)１月６日

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(72)発明者　山岡　正輝
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内
(72)発明者　小西　一也
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内
(74)代理人　弁理士　鈴木　正剛

(54)【発明の名称】　電子認証方法及びシステム

(57)【要約】
【課題】　配信側で行う情報埋め込みの前後で電子画像がさほど変化せず、受信側で適確に電子認証を行うことができる電子認証方法を提供する。
【解決手段】　配信側では、１画素が所定ビットで表現される電子画像の上位ビットからダイジェストを作成し、これを送り手の秘密鍵で暗号化して各画素の下位ビットに埋め込んでネットワークへ伝送する。受信側では、配信された電子画像から読み出した暗号ダイジェストを送り手の公開鍵で復号し、この復号したダイジェストと、配信された電子画像から直接作成した照合用ダイジェストとを比較照合し、その電子画像の真性評価を行う。



1

【特許請求の範囲】

【請求項１】　それぞれｍビットの濃度値で表現されるｎ個の画素の集合を要素単位として含む電子画像から当該電子画像の内容に関わる特定情報を作成し、作成した特定情報を公開鍵方式で暗号化して当該電子画像に埋め込む情報埋め込み過程と、

前記情報埋め込みがなされた電子画像から作成した特定情報と当該電子画像に埋め込まれた情報を復号して得られた特定情報とを比較照合することで当該電子画像の真性評価を行う認証過程とを有し、

前記情報埋め込み過程は、

前記要素単位における個々の画素の上位ｍ－ｋビットを前記特定情報の作成に用い、作成された特定情報を送り手の秘密鍵で暗号化するとともに暗号化後の情報をｎ個の画素の下位ｋビットに所定の順序情報に従って埋め込むことを特徴とする電子認証方法。

【請求項２】　前記認証過程は、前記情報埋め込みがなされた要素単位の画素の下位ｋビットを前記順序情報に従って読み出して得た暗号化後の情報を送り手の公開鍵で復号して前記特定情報を再生し、この再生された特定情報を前記情報埋め込みがなされた電子画像より作成した特定情報と比較照合することを特徴とする請求項１記載の電子認証方法。

【請求項３】　前記順序情報が、送り手と受け手との間の秘匿情報であることを特徴とする請求項１または２記載の電子認証方法。

【請求項４】　前記順序情報が、前記要素単位の構造上、一意に定められた順序に従う情報であることを特徴とする請求項１または２記載の電子認証方法。

【請求項５】　前記ｋが最低１ビットであり、前記要素単位の画素の濃度値及び画素数に応じて可変であることを特徴とする請求項１乃至４のいずれかの項記載の電子認証方法。

【請求項６】　公開鍵方式で暗号化された情報が埋め込まれた電子画像から前記情報を読み出して復号し、当該電子画像の真性評価を行う手段を備えた受信装置宛の配信情報を生成する装置であって、

それぞれｍビットの濃度値で表現されるｎ個の画素の集合を要素単位として含む電子画像を配信用画像として取り込む画像取り込み手段と、

前記配信用画像の要素単位における個々の画素の上位ｍ－ｋビットから当該配信用画像の内容に関わる特定情報を作成する情報作成手段と、

作成された特定情報を送り手の秘密鍵で暗号化する暗号化手段と、

前記暗号化手段で暗号化された情報を前記要素単位の個々の画素の下位ｋビットに所定の順序情報に従って埋め込む手段とを備えたことを特徴とする情報埋め込み装置。

【請求項７】　請求項６記載の情報埋め込み装置から情報埋め込みがなされた配信用画像を取り込む画像取り込み手段と、

情報埋め込みがなされた要素単位の画素の下位ｋビットを前記順序情報に従って読み出して前記暗号化後の情報を再構成する手段と、

再構成された前記暗号化後の情報を送り手の公開鍵で復号して前記特定情報を再生する復号化手段とを備え、

前記再生された特定情報を前記配信用画像より作成した特定情報との比較照合用の情報として保持することを特徴とする情報読み出し装置。

【請求項８】　請求項６記載の情報埋め込み装置を備えた配信装置と、請求項７記載の情報読み出し装置を備えた受信装置とを通信回線を通じて接続して構成され、

前記情報埋め込み装置から前記配信装置及び通信回線を通じて配信された前記配信用画像を前記受信装置で受信して当該配信用画像の真性評価を行うことを特徴とする電子認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、配信側で電子画像に特定情報を付加して配信し、受信側でこの特定情報を用いて当該電子画像の真性評価を行う電子認証方法及び電子認証システムに関する。

【０００２】

【従来の技術】近年、不特定多数の利用者がアクセスできるインターネット等のオープンなネットワークを通して様々な電子画像を配信及び受信する機会が増加している。ところが、こうしたオープンなネットワーク環境では、不特定多数の者が利用するため、配信途中で電子画像が第三者によって改竄され、受信者が改竄されたことに気付かない場合も想定される。また、改竄はないものの、不正に複写されて流通している場合もある。そこで、配信された電子画像が送り手から送り出されたものと同一であるか否か、或いは送り手が正当者であるか否かの確認を受信側でチェックする電子認証の仕組みが必要とされる。

【０００３】従来の電子認証の手順は、図７に示すとおりであり、配信側で、オリジナルの電子画像から作成した特定情報、例えば電子画像に対してハッシュ関数を適用してデータ圧縮したダイジェストを送り手による秘密鍵で暗号化する。そして、オリジナルの電子画像及び暗号化されたダイジェストをネットワークを通して受信側に配信する。

【０００４】受信側では、ネットワークより受信した電子画像に対してハッシュ関数によるデータ圧縮を行ってダイジェストを作成すると共に、暗号化されたダイジェストに対して送り手の公開鍵による復号化を行ってダイジェストを復号する。そして、オリジナルの電子画像から作成したダイジェストと復号したダイジェストとを比較し、両方のダイジェストが同一であれば真性な電子画

像、異なっていれば真性な電子画像ではないと判定することができる。ところで、上述のようにして電子認証を行う場合、配信側では、オリジナルの電子画像及び暗号化されたダイジェストの２種類のデータを受信側へ配信する必要があるが、電子画像が大量の場合には、ネットワークを通して配信する際に、どの電子画像に対してどのダイジェストが対応しているのかを配信側で適切に管理するためのデータ管理手段が別途必要になる。

【０００５】このようなデータ管理手段として、従来、データハイディング手法、すなわち、例えば電子文書の著作権情報をダイジェストとして暗号化し、このダイジェストをオリジナルの電子画像中に人間の目では視認できないように秘匿に埋め込んでおき、このダイジェストを必要なときに復号化して読み出す手法が採用されている。

【０００６】なお、電子画像に対する情報の埋め込み方法を採用した周知技術としては、電子画像を周波数領域に展開して特定の周波数成分に処理を施す方法を示した技術（文献「中村，小川，高嶋：ディジタル画像の著作権保護のための周波数領域における電子透かし方式，The 1997 Symposium on Cryptography and InformationSecurity-26A」に開示された技術）や、電子画像を構成する各画素の濃度値等に直接処理を施す方法を示した技術（文献「清水，沼尾，森本：ピクセルブロックによる静止電子画像データハイディング，情報処理学会第５３回全国大会2-257」に開示された技術）等が挙げられる。

【０００７】

【発明が解決しようとする課題】上述のデータハイディング手法を採用することにより、例えば、ネットワークを通して配信された電子画像から著作権情報等を受信者が容易に確認できるので、個々の電子画像とダイジェストとの関係の管理が容易になるほか、電子画像上に別途著作権表示をする必要が無くなるので、オリジナルの電子画像のまま保つことができる等の長所がある。

【０００８】しかしながら、上述のデータハンディング手法を用いて暗号化されたダイジェストを電子画像中に視認できないように秘匿に埋め込む場合、暗号化されたダイジェストの埋め込みによって電子画像自体が変化してしまうため、配信途中で改竄が無かったとしても、暗号化されたダイジェストを埋め込む前の電子画像から作成したダイジェストと埋め込んだ後の電子画像から受信側で作成したダイジェストとが著しく異なってしまい、電子認証をを適確に行うことが困難になってしまうという場合がある。

【０００９】すなわち、データハンディング手法では、一般に例えば人間の目には分り難い高周波成分を利用してダイジェストの埋め込みを行っているが、ダイジェストの作成には電子画像のビット列をバイト単位やワード単位で演算しているため、高周波成分にダイジェストを埋め込む前後で電子画像のビット列が変化し、作成されるダイジェスト自体も変化してしまう傾向がある。

【００１０】そこで本発明の課題は、適確な電子認証を可能にする改良された電子認証方法を提供することにある。本発明の他の課題は、上記電子認証方法の実施に適した電子認証システム及びその構成装置を提供することにある。

【００１１】

【課題を解決するための手段】上記課題を解決する本発明の電子認証方法は、それぞれｍビットの濃度値で表現されるｎ個の画素の集合を要素単位として含む電子画像から当該電子画像の内容に関わる特定情報を作成し、作成した特定情報を公開鍵方式で暗号化して当該電子画像に埋め込む情報埋め込み過程と、前記情報埋め込みがなされた電子画像から作成した特定情報と当該電子画像に埋め込まれた情報を復号して得られた特定情報とを比較照合することで当該電子画像の真性評価を行う認証過程とを有する。情報埋め込み過程は、前記要素単位における個々の画素の上位ｍ－ｋビットを前記特定情報の作成に用い、作成された特定情報を送り手の秘密鍵で暗号化するとともに暗号化後の情報をｎ個の画素の下位ｋビットに所定の順序情報に従って埋め込むことを特徴とする。また、前記認証過程は、前記情報埋め込みがなされた要素単位の画素の下位ｋビットを前記順序情報に従って読み出して得た暗号化後の情報を送り手の公開鍵で復号して前記特定情報を再生し、この再生された特定情報を前記情報埋め込みがなされた電子画像より作成した特定情報と比較照合することを特徴とする。

【００１２】好ましい実施の形態では、前記順序情報が、送り手と受け手との間の秘匿情報とするが、前記要素単位の構造上、一意に定められた順序に従う情報であっても良い。また、前記ｋが最低１ビットであり、前記要素単位の画素の濃度値及び画素数に応じて調整できるようにする。

【００１３】また、上記他の課題を解決する本発明の電子認証システムは、情報埋め込み装置を備えた配信装置と、情報読み出し装置を備えた受信装置とを通信回線を通じて接続し、前記情報埋め込み装置から前記配信装置及び通信回線を通じて配信された前記配信用画像を前記受信装置で受信して当該配信用画像の真性評価を行うことを特徴とする。

【００１４】配信装置側の情報埋め込み装置は、公開鍵方式で暗号化された情報が埋め込まれた電子画像から前記情報を読み出して復号し、当該電子画像の真性評価を行う手段を備えた受信装置宛の配信情報を生成する装置であって、それぞれｍビットの濃度値で表現されるｎ個の画素の集合を要素単位として含む電子画像を配信用画像として取り込む画像取り込み手段と、前記配信用画像の要素単位における個々の画素の上位ｍ－ｋビットから当該配信用画像の内容に関わる特定情報を作成する情報作成手段と、作成された特定情報を送り手の秘密鍵で暗

号化する暗号化手段と、前記暗号化手段で暗号化された情報を前記要素単位の個々の画素の下位ｋビットに所定の順序情報に従って埋め込む手段とを備えて構成される。

【００１５】また、受信装置側の情報読み出し装置は、上記情報埋め込み装置から情報埋め込みがなされた配信用画像を取り込む画像取り込み手段と、情報埋め込みがなされた要素単位の画素の下位ｋビットを前記順序情報に従って読み出して前記暗号化後の情報を再構成する手段と、再構成された前記暗号化後の情報を送り手の公開鍵で復号して前記特定情報を再生する復号化手段とを備え、前記再生された特定情報を前記配信用画像より作成した特定情報との比較照合用の情報として保持することを特徴とする。

【００１６】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して詳細に説明する。

（第１実施形態）図１は、本発明の電子認証方法の実施の形態を示した手順説明図であり、便宜上、図５に示した従来方法の手順に対応付けてある。この実施形態では、暗号化された情報、すなわち暗号ダイジェストを、以下のように電子画像に埋め込んでネットワークに配信する。

【００１７】すなわち、１画素がｍビットの濃度値で表現されるｎ個の画素の集合を要素単位として含む電子画像から個々の画素の上位ｍ－ｋビットをダイジェストの作成に用い、作成されたダイジェストを送り手の秘密鍵で暗号化して暗号ダイジェストとする。そして、この暗号ダイジェストをｎ個の画素の下位ｋビットに所定の順序情報に従って埋め込む。

【００１８】例えば、１画素の濃度値を８ビットで表現した場合、各画素を表現している最下位１ビットを変更しても人間の目にはその変化が判らないため、ダイジェストの作成には各画素を表現している１バイト（８ビット）の上位７ビットを使用し、暗号ダイジェストの埋め込みには１バイトの最下位１ビットを使用する。一方、受信側では、ネットワークを通して受信した、暗号ダイジェストが埋め込まれた電子画像に対してハッシュ関数によるデータ圧縮を行って照合用ダイジェストを作成すると共に、情報埋め込みがなされた要素単位の画素の下位ｋビットを上記順序情報に従って読み出して得た暗号ダイジェストを送り手の公開鍵で復号して元のダイジェストを再生する。そして、この再生されたダイジェストを上記照合用ダイジェストと比較照合する。順序情報は、送り手と受け手との間で定めた秘匿情報とする。

【００１９】この方法では、暗号ダイジェストを視認できないように秘匿に電子画像中に埋め込むことができるので、暗号ダイジェストを埋め込む前後で人間の目で電子画像を変化させずに電子認証を行うことが可能になる。

【００２０】（第２実施形態）次に、上述した電子認証方法を適用した電子認証システムについて説明する。この電子認証システムは、配信装置と１または複数の受信装置をそれぞれネットワークに接続し、公開鍵方式による暗号化手法を用いて電子認証を行うように構成されたものである。配信装置には本発明の情報埋め込み装置が備えられ、受信装置には、本発明の情報読み出し装置が備えられる。

【００２１】図２は、この電子認証システムの要部構成例を示したブロック図である。送信装置に備えられる情報埋め込み装置１００は、少なくとも下記機能の有するものである。

（１）それぞれｍビットの濃度値で表現されるｎ個の画素の集合を要素単位として含む電子画像を配信用画像として取り込む機能。

（２）配信用画像の要素単位における個々の画素の上位ｍ－ｋビットから当該配信用画像の内容に関わる特定情報を作成する機能。

（３）作成された特定情報を送り手の秘密鍵で暗号化する機能。

（４）暗号化された情報を要素単位の個々の画素の下位ｋビットに所定の順序情報に従って埋め込む機能。

【００２２】上記機能を実現するため、本実施形態では、画像入力部１１，電子画像蓄積部１２，データ圧縮部１３，ダイジェスト蓄積部１４，秘密鍵蓄積部１５，暗号化処理部１６，埋込処理部１７，暗号蓄積部１８，及び画像出力部１９を備えて情報埋め込み装置１００を構成している。この情報埋め込み装置１００は、例えばパーソナルコンピュータやワークステーション等の汎用コンピュータが記録媒体に記録された所定のプログラムを読み込んで実行することによって実現することができる。

【００２３】以下、配信用画像として１画素が８ビットで表わされる２５６階調のグレースケールビットマップ形式の文書画像を対象とした場合の上記情報埋め込み装置１００の動作例を具体的に説明する。この場合、各画素は０～２５５の濃度値を示す。すなわち、濃度値「０」は白画素を表わし、濃度値「２５５」は黒画素を表わし、その中間値はグレー画素を表わす。つまり、濃度値が大きい程、濃いグレー色となる。また、情報埋め込み装置１００では、上述したようにダイジェストの作成に各画素を表現している１バイト（８ビット）の上位７ビットを使用し、暗号ダイジェストの埋め込みに１バイトの最下位１ビットを使用するものとする。

【００２４】以上の前提のもと、画像入力部１１で取り込んだ、１画素が８ビットの配信用画像を画像蓄積部１２に保存させる。この後、データ圧縮部１３で画像蓄積部１２に保存された配信用画像の上位７ビットをハッシュ関数、例えば各画素の上位７ビットを１０進数に変換したものの和を２５６で除した余りを求める関数を適用

してデータ圧縮を行うことでダイジェストを作成し、このダイジェストをダイジェスト蓄積部１４に保存させる。

【００２５】次に、暗号化処理部１６で、ダイジェスト蓄積部１４に保存されたダイジェストを秘密鍵蓄積部１５内の送り手の秘密鍵により暗号化して暗号ダイジェストを生成し、これを暗号蓄積部１８に保存させる。

【００２６】埋込処理部１７では、画像蓄積部１２に保存された配信用画像の画素の最下位１ビットに所定の順序情報に従って暗号ダイジェストを埋め込み、これを画像出力部１９へ送出する。画像出力部１９では暗号ダイジェストが埋め込まれた配信用画像をネットワークＮＷへ配信する。なお、順序情報は、予め送り手と受け手との間で取り決めた秘匿情報であることが望ましいが、要素単位の構造上、その順序情報が一意に定められる場合はその順序に従っても良い。

【００２７】また、埋め込むべき暗号ダイジェストのサイズを要素単位の画素の濃度値及び画素数に応じて調整できるようにしても良い。すなわち、配送用画像が多階調のイメージ画像であり、比較的多くの下位ビットを暗号ダイジェスト用に使用しても画質の劣化が視認できない場合は、より多くの情報量をもつダイジェストを作成して埋め込むことができるようにする。

【００２８】なお、この情報埋め込み装置１００の具体的構成は一例であって、初めに説明した機能を有するものであれば他の構成であっても良い。次に、受信装置に備えられる情報読み出し装置２００について説明する。この情報読み出し装置２００は、少なくとも下記の機能を有するものである。

（１）ネットワークＮＷから情報埋め込みがなされた配信用画像を取り込む機能。

（２）情報埋め込みがなされた要素単位の画素の下位ｋビットを上記順序情報に従って読み出して暗号ダイジェストを再構成する機能。

（３）この暗号ダイジェストを送り手の公開鍵で復号して元のダイジェストを再生する機能。

（４）再生されたダイジェストを配信用画像より作成した照合用ダイジェストとの比較照合用の情報として保持する機能。

【００２９】この機能を実現するため、本実施形態では、画像入力部２１，電子画像蓄積部２２，データ圧縮部２３，ダイジェスト蓄積部２４，暗号抽出部２５，暗号蓄積部２６，復号化処理部２７，公開鍵蓄積部２８，復号化データ蓄積部２９，差分判定部３０，及び差分判定出力部３１を備えて情報読み出し装置２００を構成している。この情報読み出し装置２００は、例えばパーソナルコンピュータやワークステーション等の汎用コンピュータが記録媒体に記録された所定のプログラムを読み込んで実行することによって実現することができる。

【００３０】この情報読み出し装置２００の動作は、以下のとおりである。画像入力部２１で取り込んだ、１画素が８ビットの配信用画像（先の情報埋め込み装置１００により暗号ダイジェストが埋め込まれたもの）を画像蓄積部２２に保存させる。この後、データ圧縮部２３で画像蓄積部２２に保存された配信用画像に対してハッシュ関数を適用してデータ圧縮を行うことで照合用ダイジェストを作成し、この照合用ダイジェストをダイジェスト蓄積部２４に保存させる。

【００３１】次に、暗号抽出部２５で画像蓄積部２２に保存された配信用画像から暗号ダイジェストを読み出して暗号蓄積部２６に保存させる。復号化処理部２７は、暗号蓄積部２６に保存された暗号ダイジェストを公開鍵蓄積部２８内の送り手の公開鍵で復号して元のダイジェストを再生し、これを復号化データ蓄積部２９に保存させる。

【００３２】差分判定部３０では、ダイジェスト蓄積部２４に保存された照合用ダイジェストと復号化データ蓄積部２９に保存された元のダイジェストとを比較照合し、同一であるか否かを示す結果情報を差分判定出力部３１へ送出する。なお、この情報読み出し装置２００の具体的構成も一例であって、初めに説明した機能を有するものであれば他の構成であっても良い。

【００３３】次に、本実施形態の電子認証システムによる認証の手法を、図３及び図４を参照してより詳細に説明する。図３の情報埋め込み装置１００による１画素の濃度値を示すデータの構造例を示したものである。図３の上側のデータは「０１１１１０１１」であり、濃度値“１２３”を示している。この場合、上位７ビットの「０１１１１０１」がダイジェストの作成に利用され、最下位１ビットの「１」が暗号ダイジェストの埋め込みに利用される。図３の下側のデータは、「１１１１１１１１」で、濃度値“２５５”を示しており、この場合も、上位７ビットの「１１１１１１１」がダイジェストの作成に利用され、最下位１ビットの「１」が暗号ダイジェストの埋め込みに利用される。

【００３４】図４（ａ），（ｃ）は、配信用画像の埋め込み前後の状態推移、同（ｂ）は埋め込みの順序情報を例示したものである。ここでは、画像が３×３＝９画素で構成され、ヘッダ部分を除いたデータ部分が９バイトである配信用画像を対象としている。なお、図４（ｄ）はダイジェスト埋め込み前の各画素における濃度値、同（ｅ）は暗号ダイジェストの８ビットのデータ（ビット列のデータ）、同（ｆ）は暗号ダイジェストを埋め込んだ後の各画素における濃度値である。

【００３５】図４（ｅ）の暗号ダイジェストの８ビットデータが「０１００１０１１」であるときに埋め込みを行う場合、３×３画素の左上端画素から右方向へ、更に２行目の左端画素から右方向へと順に１画素に１ビットのデータを埋め込み、最後の右下端画素にはビット列のデータ「０１００１０１１」から算出したチェック情報

9

（チェックサムビット）を埋め込む。このチエック情報としては、例えばビット列の各ビットの和が偶数であれば「０」、奇数であれば「１」となるものを用いることができる。このように、各画素は２５６階調の濃度値で表現されており、８ビットのデータを持っているため、各画素の８ビットのデータの最下位ビットを埋め込むビット値と同じものにすることによってデータの埋め込みを行う。

【００３６】このような情報埋め込みを行えば、埋め込み前後で変換する各画素の濃度値の変化は最大で最下位の１ビット分となり、人間の目にはその相違が判別できない程度のものである。また、ハッシュ関数を適用してデータ圧縮を行ってダイジェストを作成する際、上位７ビットのみを用いることで埋め込み前の配信用画像からハッシュ関数を適用してデータ圧縮を行って作成するダイジェストと埋め込み後の配信用画像からハッシュ関数を適用してデータ圧縮を行って作成する照合用ダイジェストとを同一なものにすることが可能になる。なお、上記第２実施形態では、特定情報としてダイジェストを用いたが、他の任意の情報を用いることができることは勿論である。

【００３７】

【発明の効果】以上の説明から明らかなように、本発明によれば、暗号化後の情報を埋め込む前後で人間の目で視認できない程度の画像変化で電子認証が可能になるという特有の効果がある。また、暗号化後の情報を埋め込む前と埋め込んだ後の配信用画像から作成したダイジェスト同士を同一なものとすることができるので、適確な電子認証が可能になるという効果もある。

【図面の簡単な説明】

【図１】本発明の電子認証方法の手順説明図。

【図２】本発明の電子認証システムの要部構成例を示したブロック図。

10

【図３】本発明の電子認証システムにおいて、情報埋め込みに供される１画素の濃度値を示すデータ構造例を示した説明図。

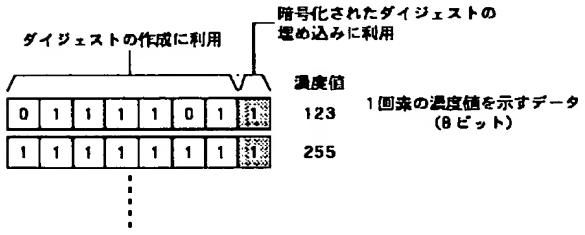
【図４】（ａ），（ｃ）は、暗号ダイジェストの埋め込み前後における配信用画像の状態推移、同（ｂ）は埋め込みの順序情報、同（ｄ）は暗号ダイジェスト埋め込み前の各画素における濃度値、同（ｅ）は暗号ダイジェストの８ビットのデータ（ビット列のデータ）、同（ｆ）は暗号ダイジェストを埋め込んだ後の各画素における濃度値の例を示した説明図。

【図５】従来の電子認証方法の手順説明図。

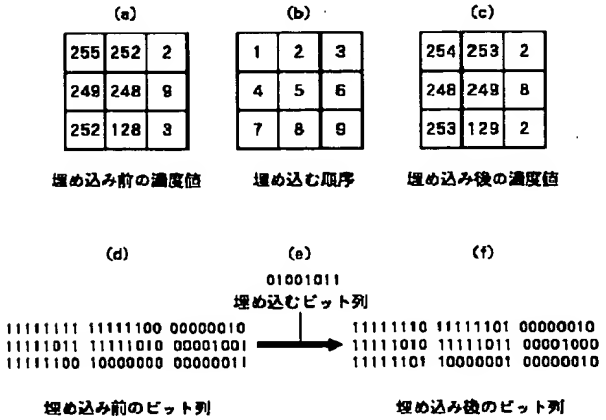
【符号の説明】

１１，２１　画像入力部
１２，２２　画像蓄積部
１３，２３　データ圧縮部
１４，２４　ダイジェスト蓄積部
１５　秘密鍵蓄積部
１６　暗号化処理部
１７　埋込処理部
１８　暗号蓄積部
１９　画像出力部
２５　暗号抽出部
２６　暗号蓄積部
２７　復号化処理部
２８　公開鍵蓄積部
２９　復号化データ蓄積部
３０　差分判定部
３１　差分判定出力部
１００　情報埋め込み装置
２００　情報読み出し装置
NWネットワーク

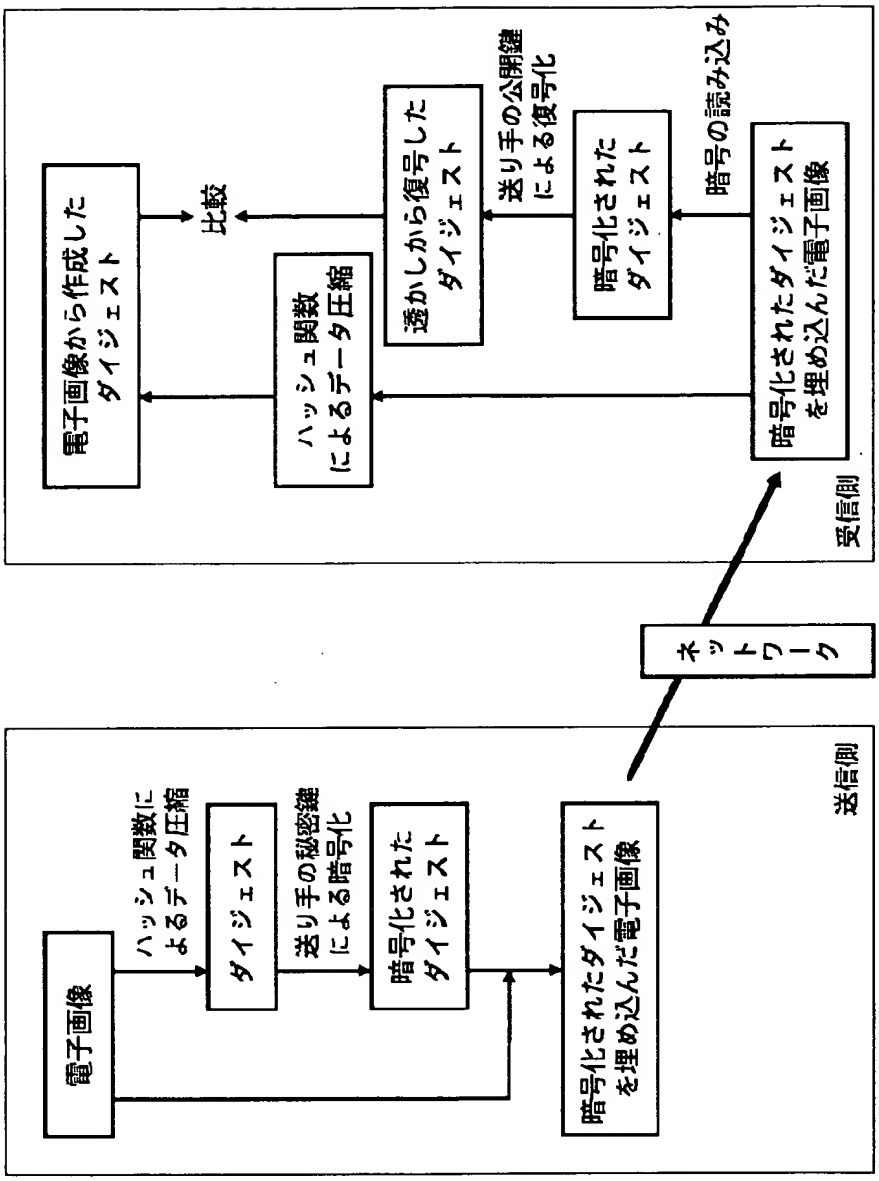
【図３】



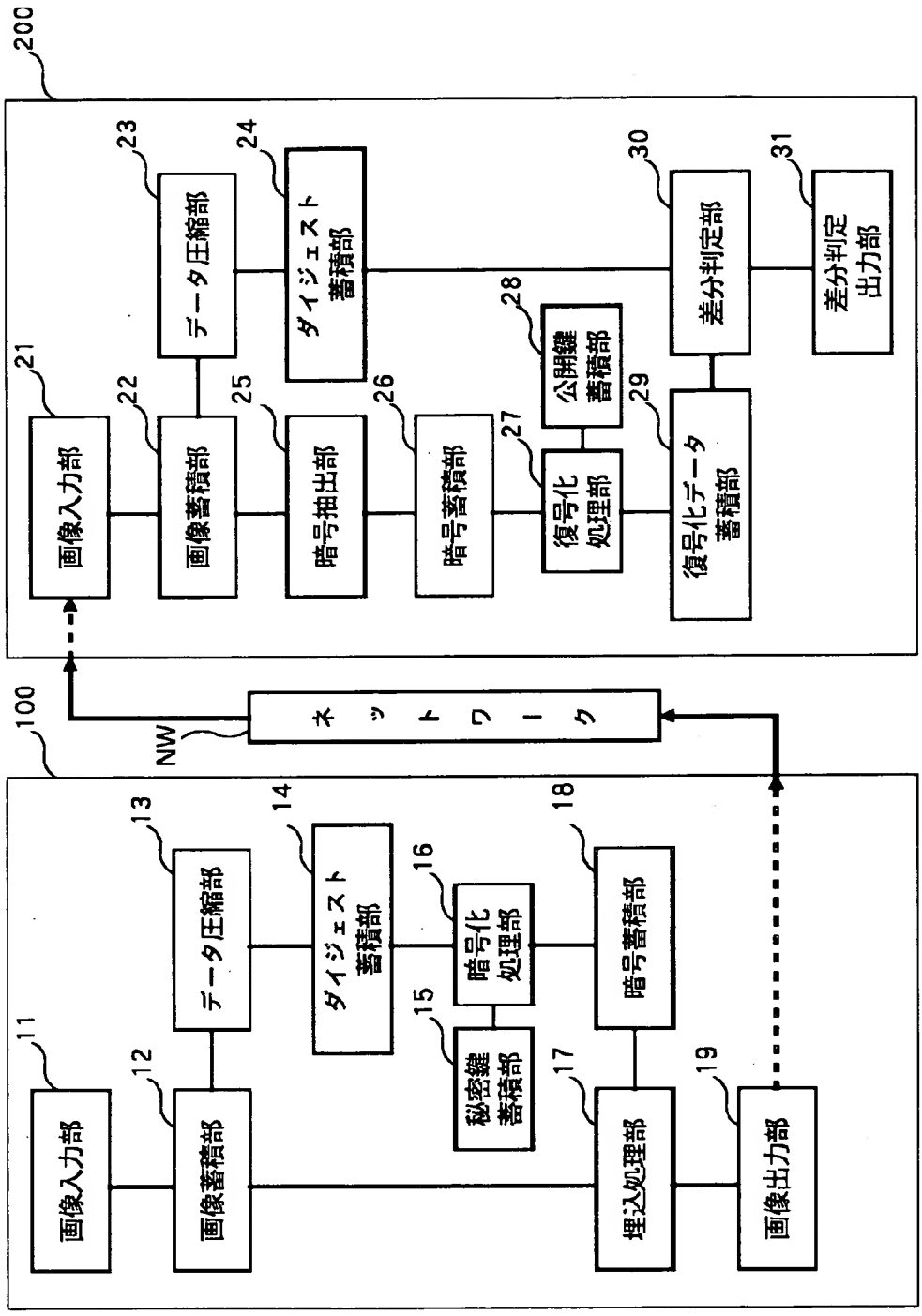
【図４】



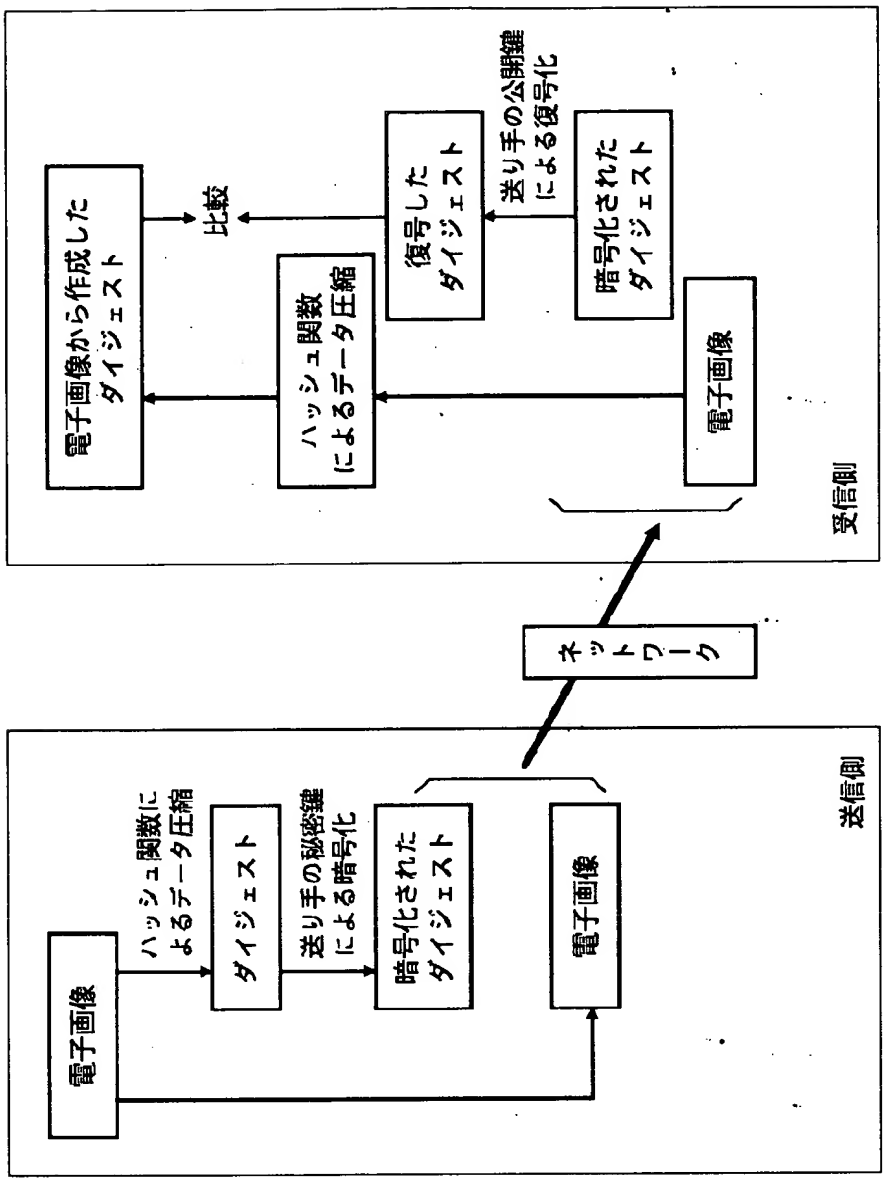
【図１】


送信側
電子画像
ハッシュ関数によるデータ圧縮
ダイジェスト
送り手の秘密鍵による暗号化
暗号化されたダイジェスト
暗号化されたダイジェストを埋め込んだ電子画像
ネットワーク
受信側
暗号化されたダイジェストを埋め込んだ電子画像
暗号の読み込み
暗号化されたダイジェスト
送り手の公開鍵による復号化
透かしから復号したダイジェスト
ハッシュ関数によるデータ圧縮
比較
電子画像から作成したダイジェスト

【図２】


200
画像入力部
21
データ圧縮部
23
ダイジェスト蓄積部
24
画像蓄積部
22
暗号抽出部
25
暗号蓄積部
26
復号化処理部
27
公開鍵蓄積部
28
復号化データ蓄積部
29
差分判定部
30
差分判定出力部
31
100
NW
ネットワーク
画像入力部
11
データ圧縮部
13
ダイジェスト蓄積部
14
暗号化処理部
16
秘密鍵蓄積部
15
暗号蓄積部
18
画像蓄積部
12
埋込処理部
17
画像出力部
19

【図５】


送信側
電子画像
ハッシュ関数によるデータ圧縮
ダイジェスト
送り手の秘密鍵による暗号化
暗号化されたダイジェスト
電子画像
ネットワーク
受信側
電子画像から作成したダイジェスト
比較
ハッシュ関数によるデータ圧縮
復号したダイジェスト
送り手の公開鍵による復号化
暗号化されたダイジェスト
電子画像